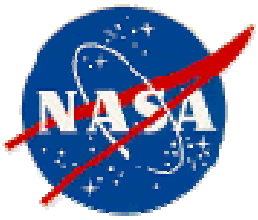

IT Security Handbook

Security Assessment and Authorization: - FIPS 199 Moderate & High Systems

ITS-HBK-2810.02-02 -
Effective Date: 20101110 -
Expiration Date: 20121110 -
Responsible Office: OCIO/ Deputy CIO for Information Technology Security

Distribution:

NODIS

Approved

Marion Meissner
Deputy Chief Information Officer for
Information Technology Security (Acting)

11/10/2010
Date

Change History

Version	Date	Change Description
1.0		Initial Version
1.1		Process refinement, grammatical
1.2		Alignment with HANDBOOK 0031
1.3	4/6/06	Process refinement, ready for final review
1.4	4/12/06	Updates per CAO telecom
1.5	5/24/06	Revised based on comments from ITSM's and CIO's
1.6	6/13/06	Formatting
2.0 (B)	1/31/07	Process adjustments and formatting
2.1 (C)	3/1/08	Process adjustments and formatting
2.2 (C)	4/1/08	Edit for structure and formatting
2.3 (C)	4/9/08	Process adjustment and formatting
2.4 (C)	6/17/08	Process adjustment
2.5	11/10/10	Update name, number, and format. System replaced with Information System as appropriate. IT replaced with Information System. Added reference to NPR 2810.1. C&A modified to read Security Assessment and Authorization. Document number changed from ITS-SOP-0030 to ITS-HBK-2810.02-02.

Table of Contents

1.0 Introduction

The NASA Security Assessment and Authorization program follows OMB and National Institute of Standards and Technology (NIST) standards and guidelines pertaining to information technology systems security. These document sets outlines the general process for achieving security assessment and authorization of Federal Government computer systems. This handbook defines the specific NASA procedure and timeline for Security Assessment and Authorization of NASA computer systems in accordance with the OMB and NIST guidance. This handbook supports implementation of requirements in *NPR 2810.1, Security of Information Technology*.

Applicable Documents

- *FIPS 199 Standards for Security Categorization of Federal Information and Information Systems.*
- *NPR 2810.1, Security of Information Technology*

2.0 Security Authorization Web Portal

The most recent version of all forms, checklists, and documentation referenced in this handbook can be located via the NASA Office of the Chief Information Officer (OCIO) website:

http://insidenasa.nasa.gov/ocio/security/CA/index.html

You are encouraged to visit the Security Assessment and Authorization Web Portal regularly to keep up-to-date with the NASA SECURITY ASSESSMENT AND AUTHORIZATION program, policies, procedures, guidance, supporting forms, and NIST documents.

3.0 Process Step Format & Acronyms

Acronyms for key individuals within the NASA security assessment and authorization process are provided below.

Step #: **[**role associated with the process step**];** details of the process step

AO	- **A**uthorizing **O**fficial
CA	- **C**ertification **A**gent
CAO	- **C**ertification and **A**ccreditation **O**fficial
CAPM	- **C**ertification and **A**ccreditation **P**rogram **M**anager
ICPM	- **I**ndependent **C**ertification **P**roject **M**anager
IDCC	- Contract managing IDCCT
IDCCT	- **I**ndependent **C**ertification **C**ontractor **T**eam
ISO	- **I**nformation **S**ystem **O**wner
ITSM	- **I**nformation **T**echnology **S**ecurity **M**anager
NSSPR	- **N**ASA **S**ystem **S**ecurity **P**lan **R**epository (currently RMS)
OC	- NSSPR **O**perations **C**enter
OCSO	- **O**rganizational **C**omputer **S**ecurity **O**fficial
PCAO	- **P**rincipal **C**ertification and **A**ccreditation **O**fficial
PM	- Independent Certification Task **P**rogram **M**anager
PO	- **P**ackage **O**wner
S-POC	- **S**ite **P**oint **O**f **C**ontact for Certification Team
VS-POC	- **V**ulnerability **S**can **P**oint **O**f **C**ontact

Figure 1 – Acronym Key

4.0 Role-Based Email Addresses

ICPM – ICPM@atlas.arc.nasa.gov

IDCC – certification-request@atlas.arc.nasa.gov

NSSPR Operational Support – CASupport@Nasa.Gov

5.0 Security Assessment and Authorization Process

5.1. **Phase I – Security Categorization & SSP Documentation:** The Security Categorization & SSP Documentation phase addresses those actions performed by the Information System Owner (ISO), Organizational Computer Security Official (OCSO), IT Security Manager (ITSM), and Certification & Accreditation Official (CAO) that categorize and generate the IT security documentation required for security assessment and authorization.

Step 1.1: **[ISO/OCSO/ITSM]**

The ISO for the system to be certified and accredited, with guidance and direction from their local OCSO and ITSM, will derive the system security categorization per ITS-HANDBOOK-0019 – "Procedure for the FIPS-199 Categorization of IT Systems", Federal Information Processing Standard (FIPS) 199, and NIST SP 800-60. Document the resulting security categorization in the "SYSTEM SECURITY CATEGORIZATION RECORD" located via the Security Assessment and Authorization Web Portal.

Guideline: The ISO should work with application owners and/or information owners to ensure that all information on the system is identified and incorporated when deriving the system security category.

Step 1.2: **[ISO]**

The ISO for the system to be certified will fill out the "REQUEST FOR CAO VALIDATION OF SECURITY CATEGORIZATION" form located via the Security Assessment and Authorization Web Portal.

Step 1.3: **[ISO]**

The ISO will E-mail the completed "REQUEST FOR CAO VALIDATION OF SECURITY CATEGORIZATION" form, the "SYSTEM SECURITY CATEGORIZATION RECORD", and any supporting documentation to the local Center CAO.

Guideline: When submitting the above forms to the CAO use the following naming conventions:

1) Name the "Subject" field of the E-mail using the following format:

Format: **CAOVR-SC:** ***<ITSSP name>***

Example: **CAOVR-SC: Code A Windows Systems**

2) Name the "SYSTEM SECURITY CATEGORIZATION RECORD" file using the following format:

Format: **SCR** ***<ITSSP name >***

Example: **SCR Code A Windows Systems**

3) - Name the "REQUEST FOR CAO VALIDATION OF SECURITY CATEGORIZATION" file using the following format:

Format: **CAOVR-SC** ***<ITSSP name>***

Example: **CAOVR-SC Code A Windows Systems**

Step 1.4: **[CAO/ITSM/OCSO/ISO/AO]**

The CAO, in coordination with the ITSM and/or OCSO, will review the submitted security categorization documentation and issue a "concur" or "non-concur" response to the ISO by completing and signing the "REQUEST FOR CAO VALIDATION OF SECURITY CATEGORIZATION".

If **Concur** response confirms the categorization and allows for the system to continue with the Security Assessment and Authorization process. Go to Step 1.5.

If **Non-Concur** response will be accompanied with a non-concur justification. The ISO then has the option to:

- Re-categorize the system based on the CAO recommendation or
- Arrange a meeting with the system Authorizing Official (AO), the CAO, OCSO, and the ITSM to determine a resolution. The certification cannot proceed until a resolution is accepted by the AO and the CAO.

Step 1.5: **[CAO/ISO/ITSM]**

- The CAO returns the approved "REQUEST FOR CAO VALIDATION OF SECURITY CATEGORIZATION" form, along with any supporting documentation, to the ISO.
- The ITSM is copied on this response so that they are notified that a new System Security Plan (SSP) certification package has been approved for generation in the NASA System Security Plan Repository (NSSPR).
- Once the certification package has been generated the ISO uploads the approved "REQUEST FOR CAO VALIDATION OF SECURITY CATEGORIZATION" form and the "SYSTEM SECURITY CATEGORIZATION RECORD" to the NSSPR as artifacts of the certification package.

Step 1.6: **[ISO/ITSM]**

The ISO will identify users who require access to the NSSPR. The ISO will apply for NSSPR accounts by completing the appropriate NSSPR ACCESS REQUEST form, located via the Security Assessment and Authorization Web Portal, and submitting it to the local Center ITSM.

Guideline: All users for whom an account is requested *must* have a current PKI certificate.

Step 1.7: **[ITSM/OC]**

ITSM will review and approve or decline account creation.

If **Approved** ITSM will email or fax the account information to the Operations Center (OC) for the NSSPR.

If **Declined** ITSM will provide justification for rejection and return the form to the requester via email or fax**.** The requester may resubmit the account request after addressing the ITSM's concerns.

Step 1.8: **[OC]**

The OC will create the accounts and send an encrypted email to the new users with their username and password within one (1) week of receipt of the NSSPR ACCESS REQUEST Form.

Step 1.9: **[ITSM]**

The ITSM will generate the SSP certification package within the NSSPR. Note that the ITSM can delegate this portion of the process to the ISO, OCSO, a local Security Assessment and Authorization plan writing team, or anyone else they deem appropriate for this role.

Requirement: When generating the SSP certification package the following naming convention is a NASA procedural requirement:

Format: ***<ITS-HANDBOOK-0007 System Designation> <System Name>***

Example: **AR-999-L-ARC-0103 Code A Windows Systems**

Step 1.10: **[ISO/ITSM/OCSO]**

The ISO, with guidance and direction from their local ITSM via their OCSO, populates the System Security Plan (SSP) certification package within the NSSPR.

Guideline: Once an SSP certification package is created, the ISO will continue populating it using the template, formats, requirements, etc. that were in effect at the time the certification package was created. Version numbers of templates or requirements used should be clearly noted where relevant in the SSP certification package. If a template or requirements change during this process, compliance with new requirements or formats should be noted as a required action in the system's Plan of Actions and Milestones (POA&M), with a completion date of no later than one year from the date of the system's new Authorization to Operate.

Step 1.11: **[ISO/OCSO]**

The ISO, in coordination with the OCSO, uses the "CERTIFICATION PACKAGE REVIEW CHECKLIST" (CPRC), downloaded via the Security Assessment and Authorization Web Portal, to verify that the package is ready for Certification Review. If any significant issues exist they must be corrected prior to continuing the Certification Review process. Minor issues can be documented in the Checklist with recommendations for correction. The "CERTIFICATION PACKAGE REVIEW CHECKLIST" is then uploaded to the NSSPR as an artifact of the certification package.

Guideline: Prior to uploading the above form to the NSSPR name the file using the following naming conventions:

Format: **CPRC** ***<ITS-HANDBOOK-0007 System Designation> <System Name>***

Example: **CPRC AR-999-L-ARC-0103 Code A Windows Systems**

Step 1.12: **[ISO/CAO]**

The ISO notifies the CAO via E-mail that the package is ready for Certification Review.

Guideline: When submitting the above notification to the CAO use the following naming convention:

Name the "Subject" field of the E-mail using the following format:

Format: **CPRC:** ***<ITS-HANDBOOK-0007 System Designation> <System Name>***

Example: **CPRC: AR-999-L-ARC-0103 Code A Windows Systems**

5.2. **Phase II – Information System Security Documentation Preliminary Review:** The IT SSP Preliminary Review phase addresses those actions performed by the CAO associated with reviewing the SSP certification package to ensure that all required IT Security documentation has been generated properly and is complete.

Step 2.1: **[CAO]**

The CAO logs into the NSSPR and, using the "CERTIFICATION PACKAGE REVIEW CHECKLIST" submitted by the ISO, verifies that the certification package meets requirements. The CAO documents any variances in the "Certification Review Variance Dispositioning" section of the CPRC.

Step 2.2: **[CAO]**

Is the Certification Package acceptable for continued processing?

If **Yes** - go to Step 3.1

If **No** - go to Step 2.3

Guideline: At this point in the process, if time constraints are tight towards meeting ATO deadlines, the remainder of Phase 2.0 can be performed in parallel with Phases 3.0 and 4.0. In cases such as this only "significant variances" should prevent the initiation of the "Independent Certification Contract" in Phase 3.0 and the subsequent "SSP Review" process in Phase 4.0. Being that the SSP Review phase primarily concerns an initial review of the SP 800-53 controls suite a gross lack of proper documentation relative to the control suite would be an example of a significant variance that could prevent continued processing.

Resolution of other identified variances contained within the larger scope of the SSP, as documented in the "CERTIFICATION PACKAGE REVIEW CHECKLIST", should be worked concurrently with Phases 3.0 and 4.0. The goal is the generation of an SSP that is as compliant as possible with policy, procedures, standards, and guidelines, prior to the IDCCT visiting the site as outlined below in Phase 6.0.

Step 2.3: **[CAO/ISO]**

The CAO notifies the ISO that the Certification Package is not acceptable for continued certification processing and instructs the ISO to correct variances per instruction the CAO has documented in the "CERTIFICATION PACKAGE REVIEW CHECKLIST".

Step 2.4: **[ISO]**

ISO corrects variances per instructions from CAO, completes the "Certification Review Variance Dispositioning" section of the CPRC, and returns it to the CAO.

Step 2.5: **[ISO/CAO]**

The ISO notifies the CAO that the variances have been corrected and the package is ready to resume the Certification Review process.

Step 2.6: **[CAO]**

The CAO verifies that the variances have been corrected. Is the Certification Package acceptable for continued processing?

If **Yes** - go to Step 3.1

If **No** - go to Step 2.3

If No agreement can be reached go to Step 2.7

Step 2.7: **[ISO/CAO/ITSM/AO]**

In the event that an agreement cannot be reached between the ISO and the CAO concerning the acceptability of the Certification Package, the ISO will arrange a meeting between the ISO, CAO, ITSM, and AO (at a minimum) to determine how to proceed. The AO is required to make a decision about whether to continue the certification process with or without addressing the CAO concerns.

- If AO chooses to not address CAO concerns, the CAO will document the decision, receive a signature of the decision from the AO on the CPRC, and upload the documented decision and CPRC as artifacts to the SSP certification package – proceed to Step 3.1

- If AO chooses to address CAO concerns – go to Step 2.3.

5.3. - **Phase III – Independent Certification Contract Initiation:** The Independent Certification Contract Initiation phase addresses those actions performed by the ISO and others to initiate the contract that processes the independent certification of the IT System.

Step 3.1: **[ISO]**

The ISO completes the SSP Certification Package. The ISO downloads the following Security Assessment and Authorization E-Forms via the Security Assessment and Authorization Web Portal:

- SYSTEM SIZING AND PRICING DOCUMENT
- PRE-ASSESSMENT CHECKLIST FOR SYSTEM OWNER

Step 3.2: **[ISO]**

The ISO completes the SYSTEM SIZING AND PRICING DOCUMENT using instructions contained within the form. For further clarification pertaining to the SYSTEM SIZING AND PRICING DOCUMENT the ISO should seek guidance from their local CSO, ITSM, or CAO.

Step 3.3 [ISO]

The ISO completes the "PRE-ASSESSMENT CHECKLIST FOR SYSTEM OWNER".

Step 3.4 [ISO/CAO]

ISO submits completed SYSTEM SIZING AND PRICING DOCUMENT and PRE-ASSESSMENT CHECKLIST FOR SYSTEM - OWNER to CAO via E-mail. -

Guideline: When submitting the above forms to the CAO use the following naming conventions: -

1) Name the "Subject" field of the E-mail using the following format: -

   Format: **PACISO: <ITS-HANDBOOK-0007 System Designation> <System Name>**

   Example: **PACISO: AR-999-L-ARC-0103 Code A Systems**

2) Name the "SYSTEM SIZING AND PRICING DOCUMENT" file using the following format:

   Format: **SSPD <ITS-HANDBOOK-0007 System Designation> <System Name>**

   Example: **SSPD AR-999-L-ARC-0103 Code A Systems**

3) Name the "PRE-ASSESSMENT CHECKLIST FOR SYSTEM OWNER" file using the following format:

Format: **PACISO <ITS-HANDBOOK-0007 System Designation> <System Name>**

Example: **PACISO AR-999-L-ARC-0103 Code A Systems**

Step 3.5 [ISO/ICPM/IDCC]

The ISO identifies funding for the assessment and ensures a transfer of the funding (via NASA Form 506) to the "IT Certification & Accreditation Project" via the "Independent Certification Project Manager (ICPM)". Work cannot begin until the funds have been received.

Step 3.6 [CAO]

The CAO completes the "PRE-ASSESSMENT CHECKLIST FOR CAO".

Step 3.7 [CAO/IDCC]

The CAO reviews the PRE-ASSESSMENT CHECKLIST FOR ISO for accuracy and submits both pre-assessment checklists (CAO and ISO versions), the SYSTEM SIZING AND PRICING DOCUMENT, and the SSP number for the system to be certified, to the IDCC via an encrypted email submission.

Guideline: When submitting the above forms to the IDCC use the following naming conventions:

1) - Name the "Subject" field of the E-mail using the following format:

Format:

IDCC: <Center Code> <ITS-HANDBOOK-0007 System Designation> <System Name>

Example: **IDCC: ARC AR-999-L-ARC-0103 Code A Systems**

2) - Ensure that the name for the "SYSTEM SIZING AND PRICING DOCUMENT" file uses the following format:

Format: **SSPD <ITS-HANDBOOK-0007 System Designation> <System Name>**

Example: **SSPD AR-999-L-ARC-0103 Code A Systems**

3) - Ensure that the name for the "PRE-ASSESSMENT CHECKLIST FOR SYSTEM OWNER" file uses the following format:

Format: **PACISO <ITS-HANDBOOK-0007 System Designation> <System Name>**

Example: **PACISO AR-999-L-ARC-0103 Code A Systems**

4) Ensure that the name for the "PRE-ASSESSMENT CHECKLIST FOR CAO" file uses the following format:

Format: **PACCAO <ITS-HANDBOOK-0007 System Designation> <System Name>**

Example: **PACCAO AR-999-L-ARC-0103 Code A Systems**

Step 3.8 [IDCC/IDCCT]

IDCC receives the CAO and ISO pre-assessment checklists and forwards them to the IDCCT as advance notification of pending assessment. No Independent Certification Review action will be taken until IDCC receives funding for the certification and issues the task order to the IDCCT. The pre-assessment checklists are being provided to the IDCCT for planning purposes only.

Step 3.9: [IDCC/ISO/ICPM/IDCCT]

IDCC provides **not-to-exceed** labor and travel cost to the ICPM, ISO, and the IDCCT.

Step 3.10: [IDCC/IDCCT]

When funding is received for the certification IDCC issues a Task Order to the IDCCT for Independent Certification review of the identified system.

5.4. - **Phase IV – SSP Review:** The SSP Review phase addresses those actions performed by the IDCCT Team associated with reviewing the SSP, developing the Security Assessment Plan and associated procedures, validating the not-to-exceed labor and travel amount specified in the Task Order, validating the sampling proposal if included, and coordinating the site visit activities with the ISO and CAO.

Step 4.1: **[ISO/PO]**

The IDCCT Team Lead makes initial contact with ISO providing ISO with the NSSPR Domain Auditor User Name with whom the package owner will share the Certification Package. The ISO contacts the package owner and requests sharing of the package with the Domain Auditor User Name account.

Guideline: The "package owner" can be the local Center ITSM or a designee of the ITSM. This is strongly recommended as it will ensure uniformity of certification packages within the NSSPR.

Step 4.2: **[IDCCT]**

The IDCCT Team Lead logs into NSSPR and performs an initial review of the SSP.

Step 4.3: **[IDCCT/ISO/CAO]**

During the initial review of the SSP the IDCCT Team Lead will be in contact with the ISO and CAO to:

- Clarify technical issues documented in the SSP
- Discuss tentative site visit dates
- Discuss tentative interview schedules
- Respond to ISO questions and concerns

Step 4.4: **[IDCCT]**

Once the Team Lead has completed their review of the SSP, the Team Lead prepares the "SSP Review Summary Report" providing feedback on the SSP, as well as providing reasonable assistance and recommendations as necessary to move the project to the on-site assessment phase. The SSP Review Summary Report must contain a statement indicating that **the Certification Package as submitted IS or IS NOT adequate for entering into the on-site assessment phase**. If not adequate for entering into the on-site assessment phase, the SSP Review Summary Report must state specific items that need to be added, modified, or corrected in the SSP to permit entering into the on-site assessment phase. The Team Lead should communicate this information to the ISO, in an effort to proactively resolve the discrepancies, before the package is kicked back to the IDCC.

Step 4.5: **[IDCCT]**

Is the Certification Package acceptable for continued processing and transition to the on-site assessment phase?

If **Yes** - go to Step 4.7.

If **No** - go to Step 4.6.

Step 4.6: **[IDCCT/IDCC/ISO]**

The Independent Certification Task **P**rogram **M**anager (PM) notifies IDCC that the Certification Package is not acceptable for continued processing and provides IDCC with the SSP Review Summary Report which states specific

items that need to be added, modified, or corrected in order to continue the independent certification review process. Processing activity will resume at Step 4.2 once the ISO has made the required modifications. The ISO may update the SSP and resubmit the SSP for review at no additional charge. The contract does allow a second review if necessary. **There is an additional charge for a third review if recertification becomes necessary.**

Step 4.7: **[IDCCT]**

The Team Lead will prepare a Security Assessment Plan (SAP) with assessment procedures in NSSPR. This plan will document the steps required to certify the identified system, the individuals involved in that process, their roles and responsibilities, and the proposed schedule.

Step 4.8: **[IDCCT/ISO/IDCC]**

The Team Lead drafts a Letter of Transmittal to the IDCC and ISO advising that the SSP Review Summary Report and the SAP with procedures are in the NSSPR. A PDF copy of the letter of transmittal is sent by E-mail to the IDCC and the ISO.

5.5. **Phase V – Assessment Preparation:** The Assessment Preparation phase addresses those actions performed by the IDCCT Team Lead in preparing for the site visit and the on-site assessment of the information system.

Step 5.1: **[IDCCT/S-POC/VS-POC]**

Once all Phase IV SSP Review activities have been completed, and the IDCCT has an acceptable Certification Package and a mutually agreed to **not-to-exceed** labor and travel cost estimate, the Team Lead proceeds with travel arrangements as follows:

- Pass team member names and visit request information to the "Site POC for the Certification Team (S-POC)" as identified in the PRE-ASSESSMENT CHECKLIST FOR CAO.
- Reconfirm dates with ISO.
- Confirm interview schedule dates and times.
- Confirm availability of documents requested in the SAP.
- Schedule vulnerability scan with the "POC for Vulnerability Scans (VS-POC)" as identified in the PRE-ASSESSMENT CHECKLIST FOR CAO. Vulnerability scans must use Agency approved vulnerability assessment tools and be scheduled no earlier than 72 hours prior to team arrival.

5.6. - **Phase VI – Security Test and Evaluation (ST&E):** The Security ST&E phase addresses those actions performed by the IDCCT Team during the on-site assessment of the information system.

Step 6.1: **[IDCCT/ISO/S-POC]**

The Team Arrives on site

Step 6.2: **[IDCCT/ISO/CAO/OCSO]**

The Team Lead conducts an In-Briefing outlining the schedule of events for the assessment. Suggested attendees for the In-Briefing include:

- ISO
- ISO's Staff
- OCSO responsible for system being assessed
- NASA Certified System Administrator for system being assessed
- Center CAO
- ITSM (optional)
- OSPP physical security representative (optional)
- Others at the discretion of the ISO

Step 6.3: **[IDCCT/ISO]**

The Assessment of the system begins. Team Lead will provide an informal Out-Briefing at the end of each day to the ISO to inform the ISO of the assessment team's progress, adjust schedules as required, and brief on problem areas that could be corrected prior to the Team leaving the site.

Step 6.4: **[IDCCT/ISO/CAO/OCSO]**

The Team Lead will provide a formal Out-Briefing to the ISO on the last day of the assessment. The Out-Briefing will provide a complete evaluation of variances to requirements uncovered during the assessment and provide proposed countermeasures. Variances that were remediated during the assessment will be shown as closed but will be included in the assessment report for statistical evaluation. Valid findings will be documented in the Security Assessment Report (SAR) stating all variances and non-compliance issues found during the assessment. Suggested attendees for the Out-Briefing are identical to those recommended for the In-Briefing as outlined above.

5.7. - **Phase VII – Report and Remediation:** The Report and Remediation phase addresses those actions performed by the IDCCT Team to document the results of the on-site assessment of the information system.

Step 7.1: **[IDCCT/ISO]**

The Assessment Team develops the final SAR in NSSPR documenting all variances and compliance issues found during the assessment. The report will provide recommended countermeasures for the ISO to remediate vulnerabilities, mitigate risk, and verify compliance objectives. The Executive Summary will specify one of three broad assessment outcomes as follows - "The system fully satisfies, partially satisfies, or does not satisfy the security objectives of the system security plan."

- The SAR will identify changes or modifications that need to be made to the SSP based on the assessment of the system by the Assessment Team. The ISO can review these suggested changes and make modifications to the SSP as deemed appropriate.

- The SAR will identify recommended actions to mitigate the vulnerabilities identified. Based on the ISO's and AO's acceptance of the recommended countermeasures these countermeasures can be integrated into the Plan of Actions and Milestones (POA&M) for tracking to completion.

Step 7.2: **[IDCCT]**

The PM reviews the SAR and the Certification Recommendations.

Step 7.3: **[IDCCT/ISO/CAO/IDCC]**

The PM signs the SAR and drafts the formal Certification Decision Letter. The Certification Decision Letter is uploaded into the Artifacts Directory of NSSPR as a PDF. PM notifies ISO, CAO, and IDCC via E-mail that the final SAR and formal Certification Decision Letter are finalized and available for further processing.

5.8. - **Phase VIII – Security Assessment Report (SAR) Acceptance:** The SAR Acceptance phase addresses actions performed by the ISO during their review and acceptance of the Security Assessment Report.

Step 8.1: **[ISO]**

The ISO reviews the SAR and Certification Decision letter. Does the ISO agree with the contents of the SAR and the Certification Decision Letter?

If **Yes** - SAR is completed, go to Step 9.1

If **No** - go to Step 8.2

Step 8.2: **[ISO]**

The ISO drafts a Memorandum for Record (MFR) recording the ISO's comments related to the SAR and/or the Certification Decision Letter. The MFR is uploaded into the Artifacts directory of the Certification Package.

Guideline: The ISO is not required to agree with the SAR in order for the Security Assessment and Authorization to be completed if the vulnerabilities found in the SAR are addressed to the satisfaction of the AO; either by putting corrective actions into the POA&M for future mitigation, documenting any accepted risks, or by obtaining concurrence from the AO that the identified issue(s) are not a threat to the system security.

5.9. - **Phase IX – Accreditation Package:** The Accreditation Package phase includes a review and validation of the SAR, creation of the accreditation package, and submission of the package to the AO.

Step 9.1: **[ISO]**

The ISO will review the SAR and create an accreditation package for the AO. The accreditation package includes (at a minimum):

- Executive summary to the AO: -
  - Short summary of the findings -
  - Actions taken to address findings -
  - Risks AO is accepting -
  - ISO's recommendation for ATO, IATO, or DATO -

- System Security Plan (SSP)
- Security Assessment Report (SAR)
- Plan of Actions and Milestones (POA&M)

Step 9.2: **[AO/ISO]**

The AO will review the certification package, make an accreditation decision (see NPR 2810.1A, section 14.4.3), and complete the Authorization to Operate (ATO), Interim ATO (IATO), or Denial of ATO (DATO) form available via the Security Assessment and Authorization Web Portal. The AO will then forward the accreditation decision to the ISO. Is the AO decision to operate?

If **Yes** - go to step 9.4

If **No** - go to step 9.3

Guideline: The AO may seek consultation with the ITSM, CAO, OCSO or others tangential to the Security Assessment and Authorization process, prior to making a final decision towards accreditation of the system. If so, the AO should be provided with pertinent information that details the residual risk to NASA missions, assets, or personnel associated with operation of the system.

Step 9.3: **[ISO]**

The ISO will input the decision letter into NSSPR and cease operation of the system.

Step 9.4: **[ISO]**

The ISO will input the decision letter into NSSPR and begin or continue operation of the system.

Security Assessment and Authorization Process Complete

Appendix A. Security Assessment and Authorization Web Portal

Please visit the NASA Office of the Chief Information Officer (OCIO) website for all documents referenced in this handbook. The Security Assessment and Authorization section can be accessed directly via the following link:

http://insidenasa.nasa.gov/ocio/security/CA/index.html

Appendix B. Roles and Responsibilities

OCIO Responsibilities: OCIO is responsible for developing NASA Security Assessment and Authorization policies and procedures for unclassified IT systems. In addition OCIO has responsibility for the implementation, tracking, and enforcement of Federal and NASA Security Assessment and Authorization requirements. These responsibilities include the following:

- **NASA Security Assessment and Authorization Program Management**:
  The NASA Security Assessment and Authorization Program Manager is responsible for implementing and managing the NASA Security Assessment and Authorization program, as described below, with the help of the NASA Principal Certification & Accreditation Official (PCAO), Center Certification & Accreditation Officials (CAO), Center ITSM's, and the Independent Certification Project Manager (ICPM).

- **Agency Principal Certification & Accreditation Official (PCAO):**

  - Function as lead and POC for all Center CAO's. -
  - Liaison between Agency Security Assessment and Authorization Program Manager and Center CAO's. -
  - Execute wide variety of tasks as identified and assigned by the Program Manager for Security Assessment and - Authorization.
  - Facilitates development of Agency Security Assessment and Authorization policies and procedures.
  - Lead weekly Agency Security Assessment and Authorization telecoms that address Security Assessment and Authorization related topics, issues, and concerns.
  - Manage Agency E-forms development, implementation, & maintenance integral to Security Assessment and Authorization
  - Facilitates development and management of Agency Security Assessment and Authorization web site hosted by OCIO.
  - Attend and facilitate Security Assessment and Authorization related tracts for Agency ITSM Conferences.
  - Directly or indirectly resolves Security Assessment and Authorization related issues and concerns as brought forth from various points throughout the Agency via CAO's and others tangential to the Security Assessment and Authorization process.

- **Center Certification & Accreditation Official (CAO):**
  This group is coordinated by the NASA Principal CAO who performs this function on behalf of OCIO. -

  - Management, facilitation, and tracking of all certifications and accreditations for their Center. -
  - Primary point of contact for all local Security Assessment and Authorization -related questions, issues, and concerns. -
  - Primary POC for all local RMS content change requests. -
  - Facilitate training and awareness relative to Security Assessment and Authorization requirements, procedures, and - processes.
  - Review & Validate system security categorizations.
  - Certification cost review to assure system components are in-line with independent certification cost estimates.
  - Facilitation, coordination, and POC for all independent system certifications at their Center.
  - Facilitation and coordination of communication between independent certifiers, independent certification contract, and SO's.
  - Verification of certification package including review of all Center SSP's and associated documentation for concurrence with Agency, NIST, OMB and other Federal Policies, Procedures, Standards, and Guidelines.
  - Document variances and recommended corrective measure in the Certification Package Review Checklist.
  - Facilitate generation of Plan of Action and Milestones (POA&M) in coordination with Center ITSM, SO, and AO.
  - Tracking and Review of the annual assessments of Continuous Monitoring controls.
  - Facilitate External Systems reviews and assessments.
  - Monthly (or more frequent) coordination and status meetings with Center ITSM and CIO.

- **CIO / ITSM:**
  Each Center CIO, ITSM, and CAO should work closely together to ensure questions and concerns are resolved early in the Security Assessment and Authorization process. Center CIO's, through their ITSM's, are responsible for the following:

  - Reviewing Security Assessment and Authorization documentation and decisions. -
  - Tracking the progress of systems in meeting Security Assessment and Authorization requirements. -
  - Tracking systems' Plans of Actions and Milestones (POA&M). -
  - Enforcing Security Assessment and Authorization requirements as necessary. -

- **Managing the NASA Independent Certification Contract**
- **Development and Management of Security Assessment and Authorization related handbooks**
- **Managing the "Certification and Accreditation" section of the NASA "Office of the Chief Information Officer" (OCIO) website.**
- **Managing the "NASA System Security Plan Repository" (NSSPR)**
- **Managing the Agency POA&M process and tool(s)**
- **Security Assessment and Authorization of OAIT, Multi-Program funded systems, and OCIO/Center systems** – As NASA organizations, NASA OCIO and each Center OCIO has the responsibility of meeting Security Assessment and Authorization requirements for the relevant OAIT, Multi-Program funded systems, and Center information systems.